Course Introduction

หลักสูตรนี้เราจะแนะนำการเขียนโปรแกรมที่ถูกหลักการ เน้นที่วิธีการเขียนที่สามารถใช้กับภาษาใดๆก็ได้ หลังจากจบหลักสูตรนี้คุณจะเข้าใจปัญหาที่เกิดขึ้นกับ Web Application โดยส่วนใหญ่รวมทั้งวิธีการป้องกันที่ถูกต้อง รวมทั้งปัญหาที่เกิดขึ้นกับการเขียน JavaScript ที่ไม่ถูกต้อง

Course Objectives

- เข้าใจวิธีการเขียนโปรแกรมที่ถูกต้อง
- รู้จักการเลือกวิธีการเข้ารหัสที่ถูกต้อง
- เขียน JavaScript ได้ถูกหลักการมากขึ้น
- เลือกวิธีการป้องกันปัญหาได้อย่างถูกต้องมากขึ้น
- รู้จักการ Logging และ Monitoring Application

Learning Level

- Intermediate

Course Duration

- 3 Days

Target Group

- Software Developer
- Software Engineer

Course Outline

Day 1

1. Security Concept

- OWASP Top 10
- OWASP Proactive Controls
- OWASP ASVS
- OWASP Testing Guide
- OWASP Security Principles

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

2. JavaScript Security

- Angular
- React
- Vue.js
- JavaScript debugging
- Real-time Application with socket.io

3. Client data storage

- Local storage
- Session storage
- IndexedDB
- WebSQL
- LocalForage

Day 2

4. Cross-Origin Resource Sharing (CORS)

- How to CORS work
- Enable CORS
- Add CORS middleware

5. Secure Headers project

- Strict Transport Security (HSTS)
- Content Security Policy (CSP)
- HTTP Public Key Pinning (HPKP)
- X-XSS Protection

6. Cryptography

- Offuscation (Encoding)
- Hashing
- Encryption

Day 3

7. Input validation

- Client side vs Server side Validation

- Whitelisting Concept
- Regular Expression
- Validating vs Sanitizing

8. Monitoring and Logging application

- Elasticsearch
- Logstash
- Kibana
- Beats
- Statd

Day 4

9. Authentication with JWT

- REST API Authentication options
- What is JSON Web Token (JWT)
- Generating JWTs
- Validating JWTs
- Using Claims
- Authorizing with Claims
- JWT attack vectors

10. Security threats

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control

Day 5

11. Security threats

- Security Misconfiguration
- Cross-site Scripting (XSS)
- Insecure deserialization
- Vulnerable Components

12. Tools for Testing

- Node security project (NSP)
- OWASP Dependency Check
- Manage code quality with SonarQube

Official Training Partner